Weather Information Database (WIDB)
Information Technology System Design Specification

Appendix A – Technical Requirements / Specification

This page left intentionally blank

Table of Contents

1   Introduction

Appendix A provides the technical requirements derived for those systems associated with the NOAA portion of the NextGen 4-D Weather Cube.

2   Cube Input Edge Services (CIES) Requirements

CIES requirements are addressed below.

2.1   CIES Functional Requirements

2.1.1   Architecture Requirements
- CIESs shall be based on SOA design and technology concepts wherever appropriate
- All CIESs shall be functionally and technically identical
  - All CIESs shall be based on a common set of standards
  - All CIESs shall be based on common data formats
  - All CIESs shall be based on a common data model
  - All CIESs shall be based on common file formats
  - All CIESs shall be based on common SW and services
  - All CIESs shall be based on common and consistent installation instructions
- The CIES shall support a variety of configuration approaches
  - CIESs shall support being configured as standalone.
  - CIESs shall support being configured for centralized access where multiple source systems share the same CIES concurrently.
  - CIESs shall support being configured for redundant access where multiple CIESs concurrently provide services to a single source system
- Agility
  - The CIES shall support the introduction of new datasets/products without interrupting other CIES operations.
  - The CIES shall support the modification of existing datasets/products without interrupting other CIES operations.
  - The CIES shall support the deletion of existing datasets/products without interrupting other CIES operations.
  - The CIES design shall be such as to allow for the future inclusion of exchange protocols (in place of or in addition to JMBL, WCS, WFS, WMS, etc) without requiring any impact to other portions of the CIES core logic.

2.1.2   Data Access / Storage Requirements
- Ingest from external sources

- o All CIESs shall be based on a common service adaptor interface.
- o The CIES shall perform any formatting / conversion of data required to convert the data from the common service adaptor interface format to that format required to store the data within the CIES.
- Data store management
  - o Access
    - ▪ The CIES shall store gridded data ingested from an external source in the following manner
      - **TBD** – NetCDF4 files in a TBD file directory structure
      - **TBD** – NetCDF3 files in a TBD file directory structure
      - **TBD** – GRIB2 files in a TBD file directory structure
      - **TBD** – GRIB files in a TBD file directory structure
      - **TBD** – HDF5 files in a TBD file directory structure
      - TBD – Any other gridded file format supported by the NetCDF4 API
    - ▪ The CIES shall store non-gridded data ingested from an external source in the following manner
      - **TBD -** Relational Database
    - ▪ The CIES shall store graphic/image data ingested from an external source in the following manner
      - **TBD**
    - ▪ The CIES shall store legacy binary files ingested from an external source in the following manner
      - **TBD**
    - ▪ The CIES shall support the storage of metadata describing its supported services and datasets/products.
  - o Housekeeping
    - ▪ The CIES shall provide data store management functions such as ensuring required data is archived and that "stale" data is purged as appropriate.
- Archival
  - o The CIES shall archive datasets/products for 15 days.
  - o The CIES shall provide for a method to retrieve archived datasets/products.
  - o The CIES shall archive all requests received.
  - o The CIEs shall provide for a method to retrieve archived past requests.
  - o The CIES shall archive the responses to all requests received. [**TBD** – should this be a COES requirement?]
  - o The CIES shall provide for a method to retrieve archived responses to past requests. [**TBD** – should this be a COES requirement?]

2.1.3 Request Management
- The CIES shall support the ability to handle a request/response message exchange pattern.

- The CIES shall support the ability to handle a subscription/publication message exchange pattern.
- Data access
  - For a JMBL request/response exchange – The CIES shall convert received JMBL-formatted request parameters into the appropriate query of data from its local datastore.
  - For an OGC WCS request/response exchange – The CIES shall convert received WCS-formatted request parameters into the appropriate query of data from its local datastore.
  - For an OGC WFS request/response exchange – The CIES shall convert received WFS-formatted request parameters into the appropriate query of data from its local datastore.
  - The CIES shall convert received request parameters for graphic/image data into the appropriate query of data from its local datastore.
  - The CIES shall convert received request parameters for legacy binary formatted data into the appropriate query of data from its local datastore.
  - Upon receipt of ingested data from an external source destined for subscription delivery, the CIES shall convert the required subscription data parameters into the appropriate query of data from its local datastore.
- Filtering / Subsetting
  - The CIES shall support the ability to filter data by dataset / product and data field.
  - The CIES shall support the ability to geospatially filter datasets/products based on the following constructs:
    - 3D bounding box
    - 2D bounding box
    - Point data
    - Horizontal cross section
    - Vertical cross section
    - Trajectory
    - Corridor
    - Airway
    - Sector
    - Sounding
  - The CIES shall support the ability to temporally filter datasets/products based on the following time parameters:
    - A future point in time
    - A current point in time
    - A past point in time
    - A future time range
    - A past time range
  - The CIES may provide only limited filtering for GRIB2-formatted data sets

- Transformations / derivations
  - The CIES shall support the ability to translate requested data from its locally stored format into each of the following based on the requested format:
    - Gridded
      - NetCDF4 -for WCS requests for any gridded data
      - GRIB2 – for WCS requests where original ingested data is GRIB2 formatted
      - GRIB - for JMBL requests (TBD – and others?)
    - Non-gridded
      - WXXM - for WFS requests
      - JMBL XML - for JMBL requests
    - Graphics / images
      - **TBD** format
    - Legacy binary file formats
      - **TBD** format
  - The CIES shall support the ability to transform requested gridded data into each of the following mapping projection formats based on the request:
    - Lambert Conformal
    - Lat/Long
    - Mercator
    - Stereographic
    - Polar radar
    - NAS Projection
  - The CIES shall provide for the capability to define and pre-process / filter / translate data sets deemed common and frequently requested in preparation for upcoming requests (including performing mapping projections, temporal and geospatial filtering).
  - The CIES shall support the ability to compress the requested data based on compression parameters in the request (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
  - The CIES shall support the ability to translate and re-grid the requested data to the appropriate resolution based on the request.
  - The CIES shall support the ability to perform the transformation / conversion of measurement information, including:
    - Celsius to Fahrenheit conversion
    - Altitude conversions
      - Flight level, Meter above MSL, Feet above ground level (AGL), Feet above MSL, Standard pressure
- Error handling
  - The CIES shall log any errors encountered in the processing of each request and make available an indication of such errors to be included in the resultant response.

- Response Handling
  - The CIES shall format the response to each request based on the parameters in the original request.
  - The CIES shall support the ability to return a response to a request in each of the following methods, as appropriate to the request type:
    - Data returned in reply
    - File returned with reply
    - Pointer to / location of response file returned with reply
  - The CIES shall provide in each response an error indication of any failed processing of, malformed, faulty, or otherwise unsupported request.
- Security
  - The CIES shall support the processing and management of security related aspects associated with the exchange of requests and responses.
- Priority processing
  - The CIES shall process requests based on the order of QOS priority, and then by order of receipt.
- Temporary storage management
  - The CIES shall provide a mechanism to temporarily store files generated by prior requests (e.g. for large JMBL files too large to be included in the original response) until either retrieved by the requestor, or purged automatically, whichever occurs first.
  - The CIES shall be capable of being configured to define a "staleness" timer for temporarily stored data.
  - The CIES shall time/date stamp each temporary file.
  - The CIES shall purge temporary files that exceed the configured "staleness" period.
  - The CIES shall log the details of each temporarily stored file (including if/when it was retrieved and by whom, or when the file was purged)

2.1.4   Subscription Management

- Subscription set up
  - The CIES shall support a mechanism to create or modify a subscription service for a given dataset/product and make the existence of the subscription service known.
- Subscription request handling
  - The CIES shall support the ability to process a request for establishing a subscription from a data consumer.
  - The CIES shall support the establishment of a subscription with delivery based on either when new data becomes available or based on a update frequency as defined in the subscription request from each data consumer.
  - The CIES shall support the management of a subscription for each data consumer for that duration of time as defined in the subscription request.
  - The CIES shall support the ability to process a request to modify a subscription from a data consumer.

- o The CIES shall support the ability to process a request for cancelling a subscription from a data consumer.
- Subscription scheduling / processing
  - o Upon receipt of ingested data from an external source defined for and destined for subscription delivery, the CIES shall convert the required subscription data parameters into the appropriate query of data from its local datastore.
  - o Based on a desired update frequency provided in the initial subscription request, the CIES shall convert the required subscription data parameters into the appropriate query of data from its local datastore
- Subscription delivery / storage processing
  - o The CIES shall provide a mechanism to deliver subscription data with the latency as defined in the original subscription request.
  - o The CIES shall support the ability to create a subscription delivery message destined to established subscription consumers, formatted based on the subscription data parameters.
  - o The CIES shall support the ability to create a subscription delivery notification message that requested subscription data is available for request by established subscription consumers.
  - o The CIES shall support the ability to create a subscription delivery notification message that requested subscription data is available for retrieval by established subscription consumers.
  - o The CIES shall support the ability to temporarily store subscription data information for future retrieval by established subscription consumers.
- Subscription delivery error handling
  - o The CIES shall identify any error conditions encountered while processing a subscription request.
  - o The CIES shall support the ability to identify any error conditions encountered while attempting to deliver subscription data to established subscription consumers.

2.1.5   Administrative / System Management
- Logging
  - o The CIES shall log relevant system activities including administrative user log-ins and activities performed, records of when data updates occur, and other key system operational events.
  - o The CIES shall log any detected fault or anomalous or performance impacting events.
  - o Provide ability to access / manage log contents
  - o The CIES shall allow for the capability to configure the level of logging and specifics as to what is logged.
- Administrative functions
  - o The CIES shall provide the necessary tools, interfaces, processing to configure, operate, monitor, troubleshoot, and administer the CIES.

- o The CIES shall provide a mechanism to manage administrative / operator user access accounts.
- o The CIES shall provide for the capability to configure and specify supported features and datasets/products, including feature names and descriptive metadata for each feature.
- o The CIES shall provide for the capability to configure and specify supported coverages and datasets/products, including coverage names and descriptive metadata for each coverage.
- Remote access support
  - o The CIES shall provide the ability to remotely access the CIES to perform any administrative functions required to ensure the continued operation and maintenance of the CIES.
- Change management support
  - o The CIES shall support the appropriate mechanisms to introduce new versions of products/ datasets and actual system software without the disruption of CIES service.
  - o The CIES shall support a mechanism to identify and track the evolution of software upgrades and their associated features.

2.1.6 Platform Management
- Load balancing
  - o The CIES design shall allow for the pooling of CIESs and the management of this pool of CIESs to handle the dynamic sharing of access from requesting consumer systems.
  - o The CIES shall support the ability to reroute requests to more lightly loaded CIES.
  - o The CIES shall support the ability to monitor current loading to determine if requests should be rerouted to more lightly loaded CIESs.
  - o The CIES shall support the ability to accept rerouted requests from other more heavily loaded CIES and perform all requested operations, returning the response to the requestor.
- Backup / synchronization
  - o The CIES design shall allow for the scheduled automated backup of persistent data.
  - o The CIES design shall allow for the manual initiation of backup of its persistent data.
  - o The CIES design shall allow for the restoral of persistent data previously backed up (e.g., in order to recover from a failed CIES instance).
- Redundancy Management
  - o The CIES design shall support the seamless operation / handoff to a backup CIES upon CIES fault / failure.
- Alarm notification / reporting
  - o The CIES shall provide a mechanism to notify an operator and remote monitoring systems upon detection of any fault or anomalous or performance impacting events
  - o The CIES shall provide a mechanism to generate reports presenting past fault or anomalous or performance impacting events.
- Self monitoring

- o HW monitoring
    - The CIES shall be capable of monitoring, logging, and reporting on key CIES hardware operational state changes and notable events, including data storage availability, equipment health, etc.
- o SW monitoring
    - The CIES shall be capable of monitoring, logging, and reporting on key CIES software operational state changes and notable events.
- o Performance monitoring
    - The CIES shall be capable of monitoring, logging, and reporting on key CIES performance metrics, including latency, response times, file sizes, request counts, etc.
- o Trend tracking / analysis
    - The CIES shall support the ability to automatically track performance trends, perform rudimentary analysis, and recommend potential actions to take to mitigate any potential building issues.

2.1.7   Discoverability

- The CIES shall support the ability to make available metadata addressing the services supported by the CIES and the datasets/products available from the CIES.
- The CIES shall support the ability to dynamically create and modify CIES service and dataset/product metadata.
- The CIES shall provide metadata appropriate for design-time discovery of services and datasets/products.
- The CIES shall provide metadata appropriate for run-time discovery of services and datasets/products.
- The CIES shall provide metadata using the formats provided in the NNEW Metadata Guidelines for the 4-D Weather Data Cube document.
- The CIES shall allow access to CIES service and dataset/product metadata via appropriate external requests (e.g., via WFS/WCS GetCapabilities commands, GetMetadata commands, etc)
- The CIES shall support a means to ensure consistency between metadata residing on the CIES (and accessible via such means as WFS/WCS Get Capabilities requests) and that metadata available at the Reg/Rep.
- The CIES shall support the ability to dynamically add/modify services that are available to support a given dataset/product (e.g., for the purpose of load balancing across multiple CIESs, for CIES maintenance windows, or CIES failure management) and convey the associated metadata information in a consistent means with the Reg/Rep.

2.1.8   Security Processing

- The CIES shall authenticate all users prior to processing their requests.
- The CIES shall provide non-repudiation service to users.

- The CIES shall verify systems providing datasets/products for distribution to the Cube are authorized to do so.
- Prior to replying with the requested information, the CIES shall verify that systems/consumers that request information are authorized to do so.
- The CIES shall provide for access control by service and by individual dataset/product.
- The CIES shall provide a mechanism to administer security policies.
- The CIES shall ensure the integrity of messages provided by systems providing datasets/products for distribution to the Cube
- The CIES shall ensure the integrity of messages provided by systems/consumers that request information
- The CIES shall provide for the confidentiality of its messages exchanged via the Cube.
- The CIES shall support the ability to audit the security aspects of all transactions.
- The CIES shall protect against threats to availability of its services.

2.1.9   QOS Processing

- A CIES's QOS for a given service shall be defined by the time to reply, toleration of packet loss, and throughput support.
- The CIES shall be able to configure access to individual data / services based on QOS classifications.
- The CIES shall enforce which users can access which level of QOS-defined service based on user classifications
- The CIES shall support the publishing of metadata that defines choices of transport along with QOS features for each data service provided.
- The CIES shall implement reliable messaging techniques to ensure high QOS performance is maintained.
- The CIES may include priority-based messaging in the communication transport layer
- The CIES shall perform priority packet loss management based on QOS classification.
- The CIES shall resolve contention management based on data QOS classification.
- The CIES shall support the means to monitor current performance and provide an alarm if QOS is not being met.
- In order to support QOS management, the CIES shall support the collection of the following statistics
  - Number of users, relative priorities, volume of info being requested
  - Observed and expected performance (end to end latencies, throughput, packet loss)
  - Amount of available and used resources

2.2   Interface Requirements

2.2.1   CIES - Reg/Rep Interface Requirements

- The CIES shall support a means to make metadata about the CIES and its supported datasets/products available to the NOAA Reg/Rep.

2.2.2   CIES –SSA Interface Requirements

- General
    - The CIES shall support a standard approach to exchanging data between an SSA and the CIES for each data format type.
    - The CIES shall support a limited number of interface formats to exchange data between an SSA and the CIES for each data format type.
    - The SSA – CIES interface shall support **TBD** security.
- The CIES shall support the following data formats when receiving and ingesting data from an SSA:
    - For gridded data:
        - NetCDF4
        - NetCDF3
        - GRIB2
        - GRIB
        - HDF5
        - TBD – Any other gridded file format supported by the NetCDF4 API
    - For non-gridded data
        - **TBD** (BUFR, others?)
    - For graphical data
        - **TBD**
    - For textual data
        - **TBD**
    - For legacy binary files
        - **TBD**
    - Other? **TBD**
- The CIES shall support the following exchange methods with an SSA:
    - For non-gridded data
        - WFS-Transaction - Insert
    - For gridded data
        - **TBD** (WCS-T?, FTP?)
    - For graphical data
        - **TBD**
    - For textual data
        - **TBD**
    - For legacy binary files
        - **TBD**
    - Other? **TBD**
        - SSA push to CIES with CIES autodetect
        - SSA push with SSA notification to CIES
        - CIES pull from SSA
        - SSA notification to CIES with CIES pull

2.2.3 CIES – Cube Interface Requirements

- Communications compatibility
  - The CIES shall make use of open standards when communicating with external Cube entities.
  - The CIES shall communicate via an underlying TCP/IP network.
  - The CIES shall utilize open standards for all data exchange communications.
  - The CIES shall be compatible with FAA Cube architecture components with which they must communicate (as defined in **TBD** FAA requirements documents), including:
    - Supporting common WFS and WCS versions, including NextGen specific extensions
      - WFS Extensions
        - Subscription
        - EXI support
        - Trajectory / corridor based data retrieval
      - WCS Extensions
        - Subscription
        - NetCDF4 and GRIB2 encoding extension
        - Trajectory / corridor based data retrieval
        - Forecast time support
    - Supporting WFS/WCS version negotiation
    - Supporting common coordinate reference systems
    - Supporting common messages encodings (SOAP, POX, KVP)
    - Supporting common operations (GetCapabilities, GetFeature, GetCoverage, DescribeFeature, DescribeCoverage)
    - Supporting common GML versions
    - Common metadata formats
    - Common asynchronous request / response – **TBD**
    - Common security approaches
- Protocols
  - For the exchange of non-gridded feature (point) data, the CIES shall support the following standards:
    - OGC WFS (with extensions)
    - JMBL
  - For the exchange of gridded coverage data, the CIES shall support the following standards:
    - OGC WCS (with extensions)
    - JMBL
  - For the exchange of graphics / image data, the CIES shall support the following standards:
    - **TBD** (WMS?)
  - For the exchange of data legacy binary file formats, the CIES shall support the following standards:
    - **TBD**

- Message exchanges / sequences
  - Reply / Request
    - The CIES shall support the ability to receive a request for datasets/products it has authority to issue.
    - The CIES shall return a reply for requested data in the designated format.
    - The CIES shall support the ability to deliver (push) a notification that requested data is available for retrieval by consumers.
    - The CIES shall return a reply indicating any error conditions encountered while processing a request.
  - Subscription /Publication
    - The CIES shall support the ability to receive a request for establishing a subscription from a data consumer which includes
      - Latency criteria
      - Time window of subscription (else forever)
      - Selection of desired update frequency or as soon as new data is available.
    - The CIES shall support the ability to receive a request to modify a subscription from a data consumer.
    - The CIES shall support the ability to receive a request for cancelling a subscription from a data consumer.
    - The CIES shall support the ability to deliver (push) data to established subscription consumers.
    - The CIES shall support the ability to deliver (push) a notification that requested subscription data is available for request by consumers.
    - The CIES shall support the ability to deliver (push) a notification that requested subscription data is available for retrieval by consumers.
    - The CIES shall return a reply indicating any error conditions encountered while processing a subscription request.
    - The CIES shall support the ability to deliver a message indicating any error conditions encountered while attempting to deliver subscription data to a data consumer.
    - The CIES shall support the ability to deliver a message to subscription consumers notifying them of any changes to the subscription service. [**TBD**- or is this done purely through updating the Reg/Rep?]
- CIES request requirements
  - The CIES shall support the ability to receive requests identifying the desired dataset/product being requested.
  - The CIES shall support the ability to receive requests identifying the desired message exchange pattern type (request/reply, subscription).
  - The CIES shall support the ability to receive requests identifying the desired geospatial parameters on which to perform filtering, including the following constructs:

- 3D bounding box
- 2D bounding box
- Point data
- Horizontal cross section
- Vertical cross section
- Trajectory
- Corridor
- Airway
- Sector
- Sounding

o The CIES shall support the ability to receive requests identifying the desired temporal (time-based) parameters on which to perform filtering, including the following:
- A future point in time
- A current point in time
- A past point in time
- A future time range
- A past time range
- Others

o The CIES shall support the ability to receive requests identifying the desired response format details, including:
- Desired data format, to include:
  - Gridded
    - o NetCDF4 -for WCS requests
    - o GRIB2 -for WCS requests
    - o GRIB - for JMBL requests (TBD – and others?)
  - Non-gridded
    - o WXXM - for WFS requests
    - o JMBL XML - for JMBL requests
  - Graphics / images
    - o **TBD** format
  - Legacy binary file formats
    - o **TBD** format
- Desired Reply MEP, to include
  - Data returned in reply
  - File returned with reply
  - Pointer to / location of response file returned with reply
- Desired mapping projection
  - Lambert Conformal
  - Lat/Long
  - Mercator

- Stereographic
- Polar radar
- NAS Projection
  - Desired compression (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
  - Desired resolution (where appropriate) for data
  - Desired error handling approach
  o The CIES shall support the ability to receive requests identifying Security related info associated with requestor and the data being requested.
  o The CIES shall support the ability to receive requests identifying desired QOS parameters. (**TBD** - or is this implied by the service chosen and its SLA as published in the Reg/Rep?)
  o The CIES shall support the ability to receive requests for metadata associated with the CIES services and its supported datasets/products.
  o **TBD**- Are measurement units an optional field in a request (e.g., Celsius vs Fahrenheit)?
- Reply delivery
  o The CIES shall deliver the response to each request based on the parameters in the original request.

2.2.4   CIES to CIES Interface

- The CIES shall support an interface to allow for the management of redundancy / load balancing across multiple CIESs.

2.2.5   CIES to Security Services Interface

- The CIES shall support appropriate exchanges with a NOAA Security Services manager responsible for security management functionality.

2.2.6   CIES to Mediation Services Interface - TBD

2.2.7   CIES to Admin Services Interface - TBD

2.3   CIES Performance Requirements

- Latency
  o For products with issuance periods of greater than 1 hour, the CIES design shall ensure availability, processing, and delivery meets overall system maximum response time of 120 seconds (objective) and 420 seconds (threshold).
  o For products with issuance periods of 15 minutes, the CIES design shall ensure availability, processing, and delivery meets overall system maximum response time of 60 seconds (objective) and 120 seconds (threshold).
  o For products with issuance periods of 5 minutes, the CIES design shall ensure availability, processing, and delivery meets overall system maximum response time of 30 seconds (objective) and 60 seconds (threshold).

- o For products with issuance periods of 1 minute, the CIES design shall ensure availability, processing, and delivery meets overall system maximum response time of 5 seconds (objective) and 30 seconds (threshold).
- Storage
  - o The CIES design shall allow for the storage of all current datasets/products, as well as archived datasets/products, requests, responses, and other persistent and temporary data required to support CIES operations and administration.
- Reliability/Availability
  - o For CIESs supporting critical NextGen services, the CIES design shall ensure overall system availability of .99999 is achieved.
  - o For CIESs supporting essential NextGen services, the CIES design shall ensure overall system availability of .999 is achieved.
  - o For CIESs supporting critical NextGen services, the CIES design shall ensure overall system MTBF of 50,000 hours is achieved.
  - o For CIESs supporting essential NextGen services, the CIES design shall ensure overall system MTBF of 5,000 hours is achieved.
  - o For CIESs supporting critical NextGen services, the CIES design shall ensure overall system MTTR of 30 minutes is achieved.
  - o For CIESs supporting essential NextGen services, the CIES design shall ensure overall system outage of less than 6 seconds is achieved.

2.4 Design Consideration Requirements

- The CIES design shall support ease of installation
- The CIES design shall be supported on both Linux and Windows platforms.
- The CIES design shall abide by the following technology standards
  - o **TBD**
- The CIES design shall make use of open standards and software wherever possible and practical.
- The CIES design shall avoid the use of COTS products (e.g. support use of PostGreSQL as opposed to Oracle) wherever possible and practical.
- The CIES design shall not disallow the potential for future public access.
- The CIES design shall consider the re-use and inclusion of the following key 3rd party developed components:
  - o NWS-developed IRIS database system (for database back-end)
  - o FAA WFS/WCS Reference Implementations
  - o JMBL Reference Implementation
  - o **TBD** AFWA WMS

3 Cube Output Edge Services (COES) Requirements

COES requirements are addressed below.

3.1   COES Functional Requirements

3.1.1   Architecture Requirements

- COESs shall be based on SOA design and technology concepts wherever appropriate
- All COESs shall be functionally and technically identical
    - All COESs shall be based on a common set of standards
    - All COESs shall be based on common data formats
    - All COESs shall be based on a common data model
    - All COESs shall be based on common file formats
    - All COESs shall be based on common SW and services
    - All COESs shall be based on common and consistent installation instructions
- The COES shall support a variety of configuration approaches
    - COESs shall support being configured as standalone.
    - COESs shall support being configured for centralized access where multiple destinations systems share the same COES concurrently.
    - COESs shall support being configured for redundant access where multiple COESs concurrently provide services to a single destination system
- Agility
    - The COES design shall be such as to allow for the future inclusion of exchange protocols (in place of or in addition to JMBL, WCS, WFS, WMS, etc) without requiring any impact to other portions of the COES core logic.

3.1.2   Storage Requirements

- Temporary storage management
    - The COES shall provide a mechanism to temporarily store files received from prior requests until either retrieved by the DSA, or purged automatically, whichever occurs first.
    - The COES shall be capable of being configured to define a "staleness" timer for temporarily stored data.
    - The COES shall time/date stamp each temporary file.
    - The COES shall purge temporary files that exceed the configured "staleness" period.
    - The COES shall log the details of each temporarily stored file (including if/when it was retrieved and by whom, or when the file was purged)
- Archival
    - The COES shall archive all requests received.
    - The COES shall provide for a method to retrieve archived past requests.
    - The COES shall archive the responses to all requests received. [**TBD** – should this be a CIES requirement?]
    - The COES shall provide for a method to retrieve archived responses to past requests. [**TBD** – should this be a CIES requirement?]

3.1.3   Request Management

- The COES shall support the ability to handle a request/response message exchange pattern.
- The COES shall perform the following sequence upon receipt of a request for data from a DSA:
    - Receive the request from the DSA and log the event
    - Perform necessary security confirmation checks to validate DSA and contents of request.
    - Return error reply if request is in error and log error event
    - Query the Reg/Rep to identify the optimal source of the requested data
    - Re-address request to identified data source
    - Apply appropriate security controls to request
    - Apply appropriate compression desires to the request (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
    - Deliver the request
    - Create a log entry for the request
- The COES shall perform the following sequence upon receipt of response to a previous request:
    - Receive the response
    - Perform necessary security confirmation checks to validate sender and contents.
    - Perform the appropriate uncompress processing to the response (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
    - Generate response addressed to originating DSA
    - Apply appropriate security controls to response
    - Deliver response to DSA
    - Create a log entry for the response
- The COES shall perform the following sequence upon receipt of notification indicating availability of requested data:
    - Receive the notification
    - Perform necessary security confirmation checks to validate sender and contents.
    - Obtain data from location identified in notification [**TBD** – need further specification on details]
    - Perform security check of retrieved file
    - Perform the appropriate uncompress processing to the response (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
    - Store data temporarily
    - Generate notification addressed to originating DSA
    - Apply appropriate security controls to notification
    - Deliver notification to DSA
    - Create a log entry for the notification
    - Perform necessary storage housekeeping to ensure temporary storage is eventually purged.

3.1.4 Subscription Management

- The COES shall support the ability to handle a subscription/publication message exchange pattern.
- The COES shall aggregate like subscription requests together (sending a single request to the Cube and identifying recipients of received subscription data and formulate the resultant reply to all aggregated DSAs.
- The COES shall perform the following sequence upon receipt of subscription request:
  - Receive the request for subscription set-up from the DSA and log the event
  - Perform necessary security confirmation checks to validate DSA and contents of request.
  - Return error reply if request is in error and log error event
  - Query the Reg/Rep to identify the optimal subscription source for the requested data (**TBD** - via out of band method?)
  - Re-address subscription request to identified source
  - Apply appropriate security controls to request
  - Apply appropriate compression desires to the request (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
  - Deliver the subscription request
  - Create a log entry for the subscription request
- The COES shall perform the following sequence upon receipt of subscription data:
  - Receive the message containing the subscription data
  - Perform necessary security confirmation checks to validate sender and contents.
  - Perform the appropriate uncompress processing to the response (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
  - Generate message containing the subscription data addressed to originating DSA
  - Apply appropriate security controls to response
  - Deliver message to DSA
  - Create a log entry for the response
- The COES shall perform the following sequence upon receipt of notification indicating availability of subscription data:
  - Receive the notification
  - Perform necessary security confirmation checks to validate sender and contents.
  - Obtain data from location identified in notification [**TBD** – need further specification on details]
  - Perform security check of retrieved file
  - Perform the appropriate uncompress processing to the response (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
  - Store data temporarily
  - Generate notification addressed to originating DSA
  - Apply appropriate security controls to notification
  - Deliver notification to DSA

- o   Create a log entry for the notification
    - o   Perform necessary storage housekeeping to ensure temporary storage is eventually purged.
- The COES shall also support the receipt and processing of messages indicating changes to an existing subscription service [**TBD** – not clear what the COES should do if notified that subscription service changes (or is removed). How does it pass this info on to something or someone that can act upon it, or at a minimum, create administrative alert / message?]

3.1.5   Discovery Management

- The COES shall support the ability to convert a received request for data from a DSA into a Reg/Rep query.
- The COES shall support the ability to receive a response from a Reg/Rep query.
- The COES shall provide a mechanism to select a single source to address a request to from a list of potential sources returned as part of the Reg/Rep query.
- The COES shall support the ability to process a response from a Reg/Rep query and convert it into the appropriate request for data from a source service identified in the response.

3.1.6   Security

- The COES shall support the processing and management of security related aspects associated with the exchange of requests and responses with the DSA and with other Cube components.

3.1.7   QOS Processing

- The COES shall be capable of being configured with user classifications that define allowable QOS levels it can request.
- The COES shall enforce which users can access which level of QOS-defined service based on user classifications
- The COES shall implement reliable messaging techniques to ensure high QOS performance is maintained.
- The COES may include priority-based messaging in the communication transport layer
- The COES shall perform priority packet loss management based on QOS classification.
- The COES shall resolve contention management based on data QOS classification.
- The COES shall support the means to monitor current performance and provide an alarm if QOS is not being met.
- In order to support QOS management, the COES shall support the collection of the following statistics
    - o   Number of users, relative priorities, volume of info being requested
    - o   Observed and expected performance (end to end latencies, throughput, packet loss)
    - o   Amount of available and used resources

3.1.8   Administrative / System Management

- Logging

- o The COES shall log relevant system activities including administrative user log-ins and activities performed, records of when data updates occur, and other key system operational events.
- o The COES shall log any detected fault or anomalous or performance impacting events.
- o Provide ability to access / manage log contents
- o The COES shall allow for the capability to configure the level of logging and specifics as to what is logged.
- Administrative functions
  - o The COES shall provide the necessary tools, interfaces, processing to configure, operate, monitor, troubleshoot, and administer the COES.
  - o The COES shall provide a mechanism to manage administrative / operator user access accounts.
- Remote access support
  - o The COES shall provide the ability to remotely access the COES to perform any administrative functions required to ensure the continued operation and maintenance of the COES.
- Change management support
  - o The COES shall support the appropriate mechanisms to introduce new versions of system software without the disruption of COES service.
  - o The COES shall support a mechanism to identify and track the evolution of software upgrades and their associated features.

3.1.9 Platform Management
- Load balancing
  - o The COES design shall allow for the pooling of COESs and the management of this pool of COESs to handle the dynamic sharing of access from requesting destination systems.
  - o The COES shall support the ability to reroute DSA requests to more lightly loaded COES.
  - o The COES shall support the ability to monitor current loading to determine if requests should be rerouted to more lightly loaded COESs.
  - o The COES shall support the ability to accept rerouted requests from other more heavily loaded COES and perform all requested operations, returning the response to the requesting DSA.
- Backup / synchronization
  - o The COES design shall allow for the scheduled automated backup of persistent data.
  - o The COES design shall allow for the manual initiation of backup of its persistent data.
  - o The COES design shall allow for the restoral of persistent data previously backed up (e.g., in order to recover from a failed COES instance).
- Redundancy Management
  - o The COES design shall support the seamless operation / handoff to a backup COES upon COES fault / failure.
- Alarm notification / reporting

- o The COES shall provide a mechanism to notify an operator and remote monitoring systems upon detection of any fault or anomalous or performance impacting events
- o The COES shall provide a mechanism to generate reports presenting past fault or anomalous or performance impacting events.
- Self monitoring
  - o HW monitoring
    - The COES shall be capable of monitoring, logging, and reporting on key COES hardware operational state changes and notable events, including data storage availability, equipment health, etc.
  - o SW monitoring
    - The COES shall be capable of monitoring, logging, and reporting on key COES software operational state changes and notable events.
  - o Performance monitoring
    - The COES shall be capable of monitoring, logging, and reporting on key COES performance metrics, including latency, response times, file sizes, request counts, etc.
  - o Trend tracking / analysis
    - The COES shall support the ability to automatically track performance trends, perform rudimentary analysis, and recommend potential actions to take to mitigate any potential building issues.

3.2 COES Interface Requirements

3.2.1 COES – Reg/Rep Interface

- The COES shall generate a Reg/Rep query with the following interface details:
  - o SOAP – based request **TBD**
- The COES shall be capable of receiving a response from a Reg/Rep query with the following interface details:
  - o SOAP – based reply **TBD**

3.2.2 DSA - COES Interface

- Communications compatibility
  - o The COES shall make use of open standards when communicating with external Cube entities.
  - o The COES shall communicate via an underlying TCP/IP network.
  - o The COES shall utilize open standards for all data exchange communications.
- Protocols
  - o For the exchange of non-gridded feature (point) data, the COES shall support the following standards:
    - OGC WFS (with extensions)
    - JMBL

- o For the exchange of gridded coverage data, the COES shall support the following standards:
  - OGC WCS (with extensions)
  - JMBL
- o For the exchange of graphics / image data, the COES shall support the following standards:
  - **TBD** (WMS?)
- o For the exchange of data legacy binary file formats, the COES shall support the following standards:
  - **TBD**
- Message exchanges / sequences
  - o Reply / Request
    - The COES shall support the ability to receive a request for datasets/products it has authority to obtain.
    - The COES shall return a reply for requested data in the designated format.
    - The COES shall support the ability to deliver (push) a notification that requested data is available for retrieval by the DSA.
    - The COES shall return a reply indicating any error conditions encountered while processing a request.
  - o Subscription /Publication
    - The COES shall support the ability to receive a request for establishing a subscription from a DSA which includes
      - Latency criteria
      - Time window of subscription (else forever)
      - Selection of desired update frequency or as soon as new data is available.
    - The COES shall support the ability to combine requests from multiple DSAa for the same data (aggregation) into a single subscription request.
    - The COES shall support the ability to receive a request to modify a subscription from a DSA.
    - The COES shall support the ability to receive a request for cancelling a subscription from a DSA.
    - The COES shall support the ability to deliver (push) data to established subscription consumers via a DSA.
    - The COES shall support the ability to deliver (push) a notification that requested subscription data is available for retrieval by consumers via the DSA.
    - The COES shall return a reply indicating any error conditions encountered while processing a subscription request from the DSA.
    - The COES shall support the ability to disaggregate subscription replies destined for multiple DSAs.
    - The COES shall support the ability to deliver a message indicating any error conditions encountered while attempting to deliver subscription data to a data consumer via the DSA.

- COES request requirements
  - The COES shall support the ability to receive requests identifying the desired dataset/product being requested.
  - The COES shall support the ability to receive requests identifying the desired message exchange pattern type (request/reply, subscription).
  - The COES shall support the ability to receive requests identifying the desired geospatial filtering parameters, including the following constructs:
    - 3D bounding box
    - 2D bounding box
    - Point data
    - Horizontal cross section
    - Vertical cross section
    - Trajectory
    - Corridor
    - Airway
    - Sector
    - Sounding
  - The COES shall support the ability to receive requests identifying the desired temporal (time-based) filtering parameters, including the following:
    - A future point in time
    - A current point in time
    - A past point in time
    - A future time range
    - A past time range
    - Others
  - The COES shall support the ability to receive requests identifying the desired response format details, including:
    - Desired data format, to include:
      - Gridded
        - NetCDF4 -for WCS requests
        - GRIB2 -for WCS requests
        - GRIB - for JMBL requests (TBD – and others?)
      - Non-gridded
        - WXXM - for WFS requests
        - JMBL XML - for JMBL requests
      - Graphics / images
        - **TBD** format
      - Legacy binary file formats
        - **TBD** format
    - Desired Reply MEP, to include

- Data returned in reply
- File returned with reply
- Pointer to / location of response file returned with reply
  - Desired mapping projection
    - Lambert Conformal
    - Lat/Long
    - Mercator
    - Stereographic
    - Polar radar
    - NAS Projection
  - Desired resolution (where appropriate) for data
  - Desired error handling approach
  - o The COES shall support the ability to receive requests identifying Security related info associated with requestor and the data being requested.
  - o The COES shall support the ability to receive requests identifying desired QOS parameters. (**TBD** - or is this implied by the service chosen and its SLA as published in the Reg/Rep?)
  - o **TBD**- Are measurement units an optional field in a request (e.g., Celsius vs Fahrenheit)?
- Reply delivery
  - o The COES shall deliver the response to each request based on the parameters in the original request.

3.2.3 COES to Cube Interface Requirements

- Communications compatibility
  - o The COES shall make use of open standards when communicating with external Cube entities.
  - o The COES shall communicate via an underlying TCP/IP network.
  - o The COES shall utilize open standards for all data exchange communications.
  - o The COES shall be compatible with FAA Cube architecture components with which they must communicate (as defined in **TBD** FAA requirements documents), including:
    - Supporting common WFS and WCS versions , including NextGen specific extensions
      - WFS Extensions
        - Subscription
        - EXI support
        - Trajectory / corridor based data retrieval
      - WCS Extensions
        - Subscription
        - NetCDF4 and GRIB2 encoding extension
        - Trajectory / corridor based data retrieval
        - Forecast time support
    - Supporting WFS/WCS version negotiation

- Supporting common coordinate reference systems
- Supporting common messages encodings (SOAP, POX, KVP)
- Supporting common operations (GetCapabilities, GetFeature, GetCoverage, DescribeFeature, DescribeCoverage)
- Supporting common GML versions
- Common metadata formats
- Common asynchronous request / response – **TBD**
- Common security approaches

- Protocols
  - For the exchange of non-gridded feature (point) data, the COES shall support the following standards:
    - OGC WFS (with extensions)
    - JMBL
  - For the exchange of gridded coverage data, the COES shall support the following standards:
    - OGC WCS (with extensions)
    - JMBL
  - For the exchange of graphics / image data, the COES shall support the following standards:
    - **TBD** (WMS?)
  - For the exchange of data legacy binary file formats, the COES shall support the following standards:
    - **TBD**
- Message exchanges / sequences
  - Reply / Request
    - The COES shall support the ability to generate a request for datasets/products it has authority to obtain.
    - The COES shall be capable of receiving a response to a request with returned data in the designated format requested.
    - The COES shall support the ability to receive a notification that data from a previous request is available for retrieval.
    - The COES shall support the ability to retrieve requested data from the designated location indicated in a received notification.
    - The COES shall be capable of processing a response indicating error conditions were encountered while processing a request.
  - Subscription /Publication
    - The COES shall support the ability to generate a request to establish a subscription which includes
      - Latency criteria
      - Time window of subscription (else forever)
      - Selection of desired update frequency or as soon as new data is available.
    - The COES shall support the ability to generate a request to modify a subscription.

- The COES shall support the ability to generate a request to cancel a subscription.
- The COES shall support the ability to receive data from a subscription source.
- The COES shall support the ability to receive a notification that subscription data is available for retrieval from subscription source.
- The COES shall support the ability to retrieve requested data from the designated location indicated in a received subscription notification
- The COES shall support the ability to process a message indicating an error condition was encountered while processing a subscription request from that COES.
- The COES shall support the ability to process a message indicating an error condition was encountered while attempting to deliver subscription data to that COES.
- The COES shall support the ability to receive a message notifying it of any changes to a subscription service. [**TBD**- or is this done purely through updating the Reg/Rep?]

- COES request requirements
  - The COES shall support the ability to generate requests identifying the desired dataset/product being requested.
  - The COES shall support the ability to generate requests identifying the desired message exchange pattern type (request/reply, subscription).
  - The COES shall support the ability to generate requests identifying the desired geospatial filtering parameters, including the following constructs:
    - 3D bounding box
    - 2D bounding box
    - Point data
    - Horizontal cross section
    - Vertical cross section
    - Trajectory
    - Corridor
    - Airway
    - Sector
    - Sounding
  - The COES shall support the ability to generate requests identifying the desired temporal (time-based) filtering parameters, including the following:
    - A future point in time
    - A current point in time
    - A past point in time
    - A future time range
    - A past time range
    - Others
  - The COES shall support the ability to generate requests identifying the desired response format details, including:
    - Desired data format, to include:
      - Gridded

- o NetCDF4 -for WCS requests
- o GRIB2 -for WCS requests
- o GRIB - for JMBL requests (TBD – and others?)
- Non-gridded
  - o WXXM - for WFS requests
  - o JMBL XML - for JMBL requests
- Graphics / images
  - o **TBD** format
- Legacy binary file formats
  - o **TBD** format
- Desired Reply MEP, to include
  - Data returned in reply
  - File returned with reply
  - Pointer to / location of response file returned with reply
- Desired mapping projection
  - Lambert Conformal
  - Lat/Long
  - Mercator
  - Stereographic
  - Polar radar
  - NAS Projection
- Desired compression (e.g. EXI compression for non-gridded data and JPEG2000 for gridded data).
- Desired resolution (where appropriate) for data
- Desired error handling approach
- o The COES shall support the ability to generate requests identifying Security related info associated with requestor and the data being requested.
- o The COES shall support the ability to generate requests identifying desired QOS parameters. (**TBD** - or is this implied by the service chosen and its SLA as published in the Reg/Rep?)
- o **TBD**- Are measurement units an optional field in a request (e.g., Celsius vs Fahrenheit)?
- Response processing
  - o The COES shall be capable of receiving a response to each request based on the parameters in the original request.

3.2.4 COES to COES Interface

- The CIES shall support an interface to allow for the management of redundancy / load balancing across multiple COESs.

3.2.5 COES to Security Services Interface

- The COES shall support appropriate exchanges with a NOAA Security Services manager responsible for security management functionality.

3.2.6 COES to Mediation Services Interface - TBD

3.2.7 COES to Administrative Services Interface - TBD

3.3 COES Performance Requirements

3.3.1 Latency

- For products with issuance periods of greater than 1 hour, the COES design shall ensure retrieval, processing, and delivery to its respective DSA meets overall system maximum response time of 120 seconds (objective) and 420 seconds (threshold).
- For products with issuance periods of 15 minutes, the COES design shall ensure retrieval, processing, and delivery to its respective DSA meets overall system maximum response time of 60 seconds (objective) and 120 seconds (threshold).
- For products with issuance periods of 5 minutes, the COES design shall ensure retrieval, processing, and delivery to its respective DSA meets overall system maximum response time of 30 seconds (objective) and 60 seconds (threshold).
- For products with issuance periods of 1 minute, the COES design shall ensure retrieval, processing, and delivery to its respective DSA meets overall system maximum response time of 5 seconds (objective) and 30 seconds (threshold).
- COES shall support the ability to handle TBD simultaneous DSA requests

3.3.2 Storage

- The COES design shall allow for the storage of archived requests, responses, and other persistent and temporary data required to support COES operations and administration.

3.3.3 Reliability/Availability

- For COESs supporting critical NextGen services, the COES design shall ensure overall system availability of .99999 is achieved.
- For COESs supporting essential NextGen services, the COES design shall ensure overall system availability of .999 is achieved.
- For COESs supporting critical NextGen services, the COES design shall ensure overall system MTBF of 50,000 hours is achieved.
- For COESs supporting essential NextGen services, the COES design shall ensure overall system MTBF of 5,000 hours is achieved.
- For COESs supporting critical NextGen services, the COES design shall ensure overall system MTTR of 30 minutes is achieved.
- For COESs supporting essential NextGen services, the COES design shall ensure overall system outage of less than 6 seconds is achieved.

3.4 Design Consideration Requirements

- The COES design shall support ease of installation
- The COES design shall be supported on both Linux and Windows platforms.

- The COES design shall abide by the following technology standards
    - **TBD**
- The COES design shall make use of open standards and software wherever possible and practical.
- The COES design shall avoid the use of COTS products (e.g. support use of PostGreSQL as opposed to Oracle) wherever possible and practical.
- The COES design shall consider the re-use and inclusion of the following key 3rd party developed components:
    - NWS-developed IRIS database system (for database back-end)
    - FAA WFS/WCS Reference Implementations
    - JMBL Reference Implementation
    - **TBD** AFWA WMS

4   Source Service Adaptor (SSA) Requirements

Source Service Adaptor requirements are addressed below.

4.1   SSA Functionality

- The SSA shall transform native (or legacy formatted) source data into a format appropriate for access by a CIES
- The SSA shall provide for the temporary storage of data while the data is waiting to be transformed, and after transformation, while the data is waiting to be moved to and ingested by the corresponding CIESs.
- An SSA shall be capable of providing transformed data to one or more CIESs.
- SSA functionality shall be capable of being performed either on a standalone platform or on a shared platform (e.g., co-located on the actual source data system, co-located on a CIES, etc.)
- The SSA shall provide sufficient administrative functionality to configure it, manage it, and monitor its operational performance.
- The SSA shall support **TBD** security.

4.2   Interfaces

4.2.1   SSA – Source System Interface Requirements

- Due to the unique nature of each source system, the interface between the SSA and each source system will likely need to be custom designed to ensure compatibility with source system.

4.2.2   SSA - CIES Interface Requirements

- General
    - The SSA shall support a standard approach to exchanging data between an SSA and a CIES for each data format type.
    - The SSA shall support a limited number of interface formats to exchange data between an SSA and a CIES for each data format type.

- o The SSA – CIES interface shall support **TBD** security.
- The SSA shall support the following data formats when providing data to a CIES for ingest:
  - o For gridded data:
    - NetCDF4
    - NetCDF3
    - GRIB2
    - GRIB
    - HDF5
    - TBD – Any other gridded file format supported by the NetCDF4 API
  - o For non-gridded data
    - **TBD** (BUFR, others?)
  - o For graphical data
    - **TBD**
  - o For textual data
    - **TBD**
  - o For legacy binary files
    - **TBD**
  - o Other? **TBD**
- The SSA shall support the following exchange methods with a CIES:
  - o For non-gridded data
    - WFS-Transaction - Insert
  - o For gridded data
    - **TBD** (WCS-T?, FTP?)
  - o For graphical data
    - **TBD**
  - o For textual data
    - **TBD**
  - o For legacy binary files
    - **TBD**
  - o Other? **TBD**
    - SSA push to CIES with CIES autodetect
    - SSA push with SSA notification to CIES
    - CIES pull from SSA
    - SSA notification to CIES with CIES pull

4.3 Performance

- SSA processing shall be fast enough as to not introduce any noticeable delay between the time the data becomes available from the source system, is transformed, and is posted to the CIES.

5   Destination Service Adaptor (DSA) Requirements

Destination Service Adaptor requirements are addressed below.

5.1   DSA Functionality

- Request management
  - The DSA shall be capable of creating a properly formatted request for desired data, including the detailed parameters describing the data (filters, message exchange pattern, etc).
  - The DSA shall handle receipt of a reply if the data request was in error or requested data was unavailable
  - The DSA shall support the generation and delivery of a request for subscription data
  - The DSA shall handle the receipt of unsolicited subscription data
  - The DSA shall handle the receipt of notification that data is available for retrieval from the COES
  - The DSA shall, upon receipt of notification that data is available, retrieve data using appropriate exchange means
- Data Transformation
  - The DSA shall transform data available from a COES into a native (or legacy formatted) format appropriate for access by a destination system
- Storage
  - The DSA shall provide for the temporary storage of data while the data is waiting to be transformed, and after transformation, while the data is waiting to be moved to the corresponding destination system.
- Architectural
  - A DSA shall be capable of obtaining data from one or more COESs to be transformed for use by its respective destination system.
  - DSA functionality shall be capable of being performed either on a standalone platform or on a shared platform (e.g., co-located on the actual destination data system, co-located on a COES, etc.)
- Administrative
  - The DSA shall provide sufficient administrative functionality to configure it, manage it, and monitor its operational performance.
- Security
  - The DSA shall support **TBD** security.

5.2   DSA Interfaces

5.2.1   DSA – Destination System Interface Requirements

- Due to the unique nature of each destination system, the interface between the DSA and each destination system will likely need to be custom designed to ensure compatibility with each destination system.

5.2.2 DSA - COES Interface Requirements

- Communications Compatibility
  - The DSA shall make use of open standards when communicating with external Cube entities.
  - The DSA shall communicate via an underlying TCP/IP network.
  - The DSA shall utilize open standards for all data exchange communications.
- Protocols
  - For the exchange of non-gridded feature (point) data, the DSA shall support the following standards:
    - OGC WFS (with extensions)
    - JMBL
  - For the exchange of gridded coverage data, the DSA shall support the following standards:
    - OGC WCS (with extensions)
    - JMBL
  - For the exchange of graphics / image data, the DSA shall support the following standards:
    - **TBD** (WMS?)
  - For the exchange of data legacy binary file formats, the DSA shall support the following standards:
    - **TBD**
- Message Exchanges / Sequences
  - Reply / Request
    - The DSA shall support the ability to generate a request for datasets/products it has authority to obtain.
    - The DSA shall be capable of receiving a response to a request with returned data in the designated format requested.
    - The DSA shall support the ability to receive a notification that data from a previous request is available for retrieval.
    - The DSA shall support the ability to retrieve requested data from the designated location indicated in a received notification.
    - The DSA shall be capable of processing a response indicating error conditions were encountered while processing a request.
  - Subscription /Publication
    - The DSA shall support the ability to generate a request to establish a subscription which includes
      - Latency criteria
      - Time window of subscription (else forever)
      - Selection of desired update frequency or as soon as new data is available.

- The DSA shall support the ability to generate a request to modify a subscription.
- The DSA shall support the ability to generate a request to cancel a subscription.
- The DSA shall support the ability to receive data from a subscription source.
- The DSA shall support the ability to receive a notification that subscription data is available for retrieval from subscription source.
- The DSA shall support the ability to retrieve requested data from the designated location indicated in a received subscription notification.
- The DSA shall support the ability to process a message indicating an error condition was encountered while processing a subscription request from that DSA.
- The DSA shall support the ability to process a message indicating an error condition was encountered while attempting to deliver subscription data to that DSA.
- The DSA shall support the ability to receive a message notifying it of any changes to a subscription service. [**TBD**- or is this done purely through updating the Reg/Rep?]

- DSA Request Requirements
  - The DSA shall support the ability to generate requests identifying the desired dataset/product being requested.
  - The DSA shall support the ability to generate requests identifying the desired message exchange pattern type (request/reply, subscription).
  - The DSA shall support the ability to generate requests identifying the desired geospatial filtering parameters, including the following constructs:
    - 3D bounding box
    - 2D bounding box
    - Point data
    - Horizontal cross section
    - Vertical cross section
    - Trajectory
    - Corridor
    - Airway
    - Sector
    - Sounding
  - The DSA shall support the ability to generate requests identifying the desired temporal (time-based) filtering parameters, including the following:
    - A future point in time
    - A current point in time
    - A past point in time
    - A future time range
    - A past time range
    - Others

- o The DSA shall support the ability to generate requests identifying the desired response format details, including:
    - Desired data format, to include:
        - Gridded
            - o NetCDF4 -for WCS requests
            - o GRIB2 -for WCS requests
            - o GRIB - for JMBL requests (TBD – and others?)
        - Non-gridded
            - o WXXM - for WFS requests
            - o JMBL XML - for JMBL requests
        - Graphics / images
            - o **TBD** format
        - Legacy binary file formats
            - o **TBD** format
    - Desired Reply MEP, to include
        - Data returned in reply
        - File returned with reply
        - Pointer to / location of response file returned with reply
        - Best attempts to deliver vs ensuring guaranteed delivery
    - Desired mapping projection
        - Lambert Conformal
        - Lat/Long
        - Mercator
        - Stereographic
        - Polar radar
        - NAS Projection
    - Desired resolution (where appropriate) for data
    - Desired error handling approach
- o The DSA shall support the ability to generate requests identifying Security related info associated with requestor and the data being requested.
- o The DSA shall support the ability to generate requests identifying desired QOS parameters. (**TBD** - or is this implied by the service chosen and its SLA as published in the Reg/Rep or controlled by the COES?)
- o **TBD**- Are measurement units an optional field in a request (e.g., Celsius vs Fahrenheit)?
- Response Processing
    - o The DSA shall be capable of receiving a response to each request based on the parameters in the original request.

5.3 Performance

- DSA processing shall be fast enough as to not introduce any noticeable delay between the time the destination system requests data and the time the request has been conveyed to the COES.
- DSA processing shall be fast enough as to not introduce any noticeable delay between the time the requested data becomes available from the COES, is transformed, and is moved to the destination system.

6 Security Services Requirements

- Detailed requirements associated with security services are in the initial stages of consideration.
- Performance requirements
  - o Security Services shall handle TBD simultaneous requests
  - o Security Services shall respond to requests within TBD time
  - o Security Services shall support TBD throughput
  - o Security Services shall add no more than TBD latency to any data

7 Registry / Repository Requirements

Registry/repository requirements are as follows:

- The Reg/Rep shall support design-time discovery of supported CIES services
- The Reg/Rep shall support design-time discovery of datasets/products for each CIES
- The Reg/Rep shall support run-time discovery of CIES services
- The Reg/Rep shall support run-time discovery of datasets/products for each CIES
- The Reg/Rep shall provide metadata descriptions about CIES services
- The Reg/Rep shall provide metadata descriptions about datasets/products for each CIES
- The Reg/Rep shall support a common metadata standard to ensure interoperability between inter-agency users.
- The Reg/Rep shall support semantically enhanced discovery of datasets/products via ontology mapping and mediation capabilities.
- All instances of the Reg/Reps shall be consistent with each other via the incorporation of a federated architecture approach.
- The Reg/Rep shall support the machine –to- machine exchange of information (used to populate its contents or to retrieve its contents for review and use)
- The Reg/Rep shall support human, real time access via the appropriate user interface to support the exchange of information (used to populate its contents or to retrieve its contents for review and use)
- The Reg/Rep shall support the receipt of queries with the following interface details:
  - o SOAP (and REST? – **TBD**)
- The Reg/Rep shall be capable of providing a query response with the following interface details:

- o SOAP (and REST? – **TBD**)
- The Reg / Rep shall store metadata in formats that abide by the following metadata standards
    - o TBD
- The Reg / Rep may support additional features including subscription, notification, versioning, and replication.
- The Reg/ Rep shall support spatial extensions to ebXML to enable spatial metadata tagging and spatial searches
- The Reg / Rep shall support fault tolerance operations via the use of an automatic failover to a chain of backup systems, if so configured.
- Performance Requirements
    - o The Reg/Rep shall support the ability to exchange data to federated Reg/Rep systems within TBD seconds.
    - o The Reg/Rep shall reply to a query within TBD seconds
    - o The Reg/Rep shall handle TBD requests per TBD timeframe without impacting response time performance

8   Mediation Services Requirements

Mediation services requirements are as follows:

- Mediation services shall perform any necessary protocol and data format translations required to support the exchange of information between non-interoperable systems.
- Mediation services shall support the translation between each of the following:
    - o JMBL GRIB and OGC WCS NetCDF4
    - o JMBL SOAP/XML and OGC WFS WXXM
    - o BUFR and WXXM
    - o GRIB2 and NetCDF4
- Performance requirements
    - o Mediation Services shall handle TBD simultaneous requests
    - o Mediation Services shall respond to requests within TBD time
    - o Mediation Services shall support TBD throughput
    - o Mediation Services shall add no more than TBD latency to any data
- Interface requirements
    - o TBD
-

9   Administrative Services Requirements

- Functional requirements - TBD

- Performance requirements - TBD

- Interface requirements - TBD

10 Remaining Requirement Issues

Numerous requirements above are still TBD. Additional concerns include:

- How will decoder metadata (e.g. BUFR tables) be handled?

- Where does uncompression take place (COES or DSA). Does DSA or COES request compression, or is it applied regardless if the metadata defines it as a compressed reply?

- What gridded file formats are supported for JMBL

- Where are the security requirements?

- What are the performance requirements?

- Support for graphical and binary formatted legacy data (formats, services, etc)